



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,496	10/29/2001	Carey Nachenberg	20423-05957	3384

45969 7590 04/10/2006

SONNENSCHN NATH & ROSENTHAL LLP
FOR SYMANTEC CORPORATION
P. O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER

WILLIAMS, JEFFERY L

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/046,496	Applicant(s) NACHENBERG ET AL.	
	Examiner Jeffery Williams	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 February 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 and 20-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 and 20-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 October 2001 is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>2/6/2006</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the communication filed on 2/6/2006.

All objections and rejections not set forth below have been withdrawn.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/6/2006 has been entered.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Applicants have amended claims 12 and 32 to include the limitations for *"a content executability determination module, coupled to the antivirus module, configured to determine the executability of the computer content in response to comparing the time stamp of the target content with the virus alert time"*, and *"and coupled to the comparing means, means for determining the executability of the computer content in response to comparing the time stamp of the target computer content with the virus alert time"*.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 12 – 17 and 32 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application

was filed, had possession of the claimed invention. For example, regarding claims 12 and 32, the specification does not describe, amongst other things, a "content executability determination module" and a "coupling" of a "comparing means" and "determining" means. See objection to specification above.

Claims 13 – 17 are rejected by virtue of dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 – 10 and 12 – 33 is rejected under 35 U.S.C. 102(e) as being anticipated by Bates et al., U.S. Patent 6,721,721 B1.

Regarding claim 1, Bates et al. discloses:
entering a first computer virus status mode in response to a first computer virus outbreak report (Bates et al., col. 1, lines 13-52). Bates et al. reports the outbreak of

1 new and more sophisticated viruses. The invention as disclosed by Bates et al. is for
2 the purpose of protecting against these outbreaks.

3 *computing a first computer virus alert time corresponding to entry into the first*
4 *computer virus status mode* (Bates et al., fig. 7, elem. 214; col. 7, lines 20-35). Herein,
5 Bates et al. discloses a method for accessing computer content on a local machine or
6 on a network. Content is filtered based upon a generated virus alert time, a rule derived
7 from relative time parameters (criterion) entered (via computer means, "computing") by
8 a user in a virus status mode. The relative time parameters (i.e. "virus found in last 7
9 days", "not checked in last 14 days") are processed ("computing") into a rule, which is
10 then utilized by the system to compare with the timestamps of content and make
11 determinations of trustworthiness (Bates et al., col. 11, lines 12-24; col. 13, lines 22-34;
12 col. 17, lines 35-49; col. 18, lines 22-30).

13 *comparing a time stamp of a computer content with the first computer virus alert*
14 *time* (Bates et al., col. 9, line 65 – col. 10, line 3; col. 11, lines 12-24; col. 12, lines 59-
15 62);

16 *and determining the executability of the computer content in response to the*
17 *result of the comparing step* (Bates et al., col. 9, line 56 – col. 10, line 8; col. 11, lines
18 12-24). Bates et al. discloses that in response to a comparison, a determination of
19 computer content executability is performed.

20
21
22 Regarding claim 2, Bates et al. discloses:

1 *receiving a first access control time based on the first virus outbreak report*
2 (Bates et al., fig. 7, elem. 214). The system of Bates et al. takes human input and
3 “automatically” generates computer readable parameters.

4 *and converting the first access control time into the first virus alert time* (Bates et
5 al., fig. 7, elem. 214; col. 12, lines 59-62). A “prior point in time” (“virus alert time”) is
6 derived from the period of time specified by element 214 (“access control time”) and is
7 compared to the timestamp of the file.

8
9 Regarding claim 3, Bates et al. discloses:

10 *wherein the first access control time is a relative time stamp* (Bates et al., fig. 7,
11 elem. 214; col. 12, lines 59-62). A “prior point in time” (“virus alert time”) is derived from
12 the period of time specified by element 214 (“access control time”) and is relative in
13 time.

14
15 Regarding claim 4, Bates et al. discloses:

16 *wherein the first access control time is a pre-determined time period for access*
17 *control under the first computer virus status mode* (Bates et al., fig. 7, elem. 214). The
18 access control time is pre-determined by the user.

19
20 Regarding claim 5, Bates et al., discloses:

21 *determining the presence of a value representing the computer content in a*
22 *memory table of executable computer content* (Bates et al., col. 7, lines 12-34).

1

2 Regarding claim 6, Bates et al., discloses:

3 *wherein the computer content is not executed when the value representing the*
4 *computer content is not present in the memory table of executable computer content*
5 (Bates et al., col. 11, lines 11-24; col. 3, lines 24-27). As disclosed by Bates et al.,
6 content not present in the memory table of executable computer content is flagged as
7 untrustworthy. The invention as disclosed by Bates et al. is configurable to eliminate
8 untrustworthy computer content from the list of accessible content, thus not providing
9 access to the content for execution.

10

11 Regarding claim 7, Bates et al. discloses:

12 *wherein the value is a hash value of the computer content* (Bates et al., col. 12,
13 lines 55-58).

14

15 Regarding claim 8, Bates et al. discloses:

16 *wherein the computer content is executed only when the computer content is*
17 *time stamped prior to the first computer virus alert time* (Bates et al., col. 13, lines 42-
18 59; col. 3, lines 24-27). Computer content that is time stamped prior to the first
19 computer virus alert time is branded as trustworthy. Thus, the content would not be
20 subjected to denial of access for execution.

21

22 Regarding claim 9, Bates et al. discloses:

1 *entering types of computer codes that should be blocked from execution in*
2 *response to the first computer virus outbreak report* (Bates et al., col. 9, line 62 – col.
3 10, line 28);

4 *and blocking execution of a computer code that belongs to the entered types of*
5 *computer codes* (Bates et al., col. 3, lines 24-27). The invention as disclosed by Bates
6 et al. is configurable to eliminate untrustworthy computer content from the list of
7 accessible content, thus not providing access to the content for execution.

8
9 Regarding claim 10, Bates et al. discloses:

10 *generating a second virus alert time in response to a second computer virus*
11 *outbreak report; comparing the time stamp of the computer content with the second*
12 *computer virus alert time; determining the executability of the computer content in*
13 *response to the result of comparing the time stamp of the computer content with the*
14 *second computer virus alert time* (Bates et al., col. 3, lines 5 – 15). The above
15 limitations of claim 10 are essentially similar to claim 1 with the exception that they are
16 directed to a second instance of the method of claim 1. Bates et al. discloses that the
17 method of claim 1 produces a set of results. Thus, Bates et al. discloses a secondary
18 instance of the method of claim 1, as the word “set” dictates more than a singular
19 occurrence of the method of claim 1.

20 *performing antivirus processing upon the computer content* (Bates et al., col. 9,
21 lines 62-66). Bates et al. discloses the processing of computer content for the likelihood
22 of existing viruses.

1

2 Regarding claim 12, Bates et al. discloses:

3 *an access control console, for entering a first computer virus status mode and for*
4 *recovering a preselected virus access control time corresponding to said virus status*
5 *mode* (Bates et al., fig. 1, elem. 33; fig. 7);

6 *an anti-virus module, coupled to the access control console, configured to*
7 *compute a virus alert time based on the virus access control time and to compare a time*
8 *stamp of a target computer content with the virus alert time prior to execution of the*
9 *target computer content* (Bates et al., fig. 1, elem. 30; see rejections of claims 1 and 2).

10 *and a content executability determination module, coupled to the anti-virus*
11 *module, configured to determine the executability of the computer content in response*
12 *to comparing the time stamp of the target computer content with the virus alert time*
13 (Bates et al., col. 9, line 56 – col. 10, line 8; col. 11, lines 12-24). Bates et al. discloses
14 that in response to a comparison, a determination of computer content executability is
15 performed. Thus Bates discloses *content executability determination module*, a
16 functional module logically coupled to the system comprising an *anti-virus module*, used
17 to determine the trustworthiness (“executability”) of content.

18

19 Regarding claim 13, Bates et al. discloses:

20 *a memory module for storing time stamps of the plurality of computer contents*
21 (Bates et al., fig. 1, elem. 46);

Art Unit: 2137

1 *and an access control module, coupled to the access control console and to the*
2 *memory module, for computing the virus alert time and for comparing the time stamp of*
3 *each target computer content with the virus alert time (Bates et al., fig. 1, elem. 42; see*
4 *rejections of claims 1 and 2).*

5
6 Regarding claim 14, Bates et al. discloses:

7 *a computer virus processing module, coupled to the access control module, for*
8 *further processing a target computer content in order to determine the executability of*
9 *the target computer content (Bates et al., fig. 1, elem. 44).*

10
11 Regarding claim 15, Bates et al. discloses:

12 *wherein the memory module stores a value representing each of the computer*
13 *contents (Bates et al., col. 12, lines 52-65).*

14
15 Regarding claim 16, Bates et al. discloses:

16 *wherein the access control module is configured to determine the presence of*
17 *the value in the memory module as representing a target computer content (Bates et al.,*
18 *fig. 3).*

19
20 Regarding claim 17, Bates et al. discloses:

21 *wherein the value is a hash value (Bates et al., col. 12, lines 52-65).*
22

Art Unit: 2137

1 Regarding claim 20, Bates et al. discloses:

2 *creating a list of time-stamped executable computer contents* (Bates et al., fig. 3,
3 elem. 92).

4 *entering a virus alert mode in response to a virus outbreak report* (Bates et al.,
5 fig. 2; col. 1, lines 13-52).

6 *responsive to the virus alert mode, entering an access control message for*
7 *specifying an access control rule for blocking the execution of suspicious or susceptible*
8 *computer contents that are time-stamped not before computed virus alert time, the*
9 *access control message including a first control parameter for computing the virus alert*
10 *time* (Bates et al., fig. 2; fig. 7; see rejections of claims 1 and 2).

11 *receiving a request to execute a target computer content; and determining the*
12 *executability of the target computer content based on the access control rule in the*
13 *access control message* (Bates et al., fig. 2).

14
15 Regarding claim 21, Bates et al. discloses:

16 *applying anti-virus operation upon each executable computer content, storing a*
17 *hash value of each executable computer content in the list; and inserting a time stamp*
18 *corresponding to the moment of storing the hash value of the executable computer*
19 *content* (Bates et al., fig. 3).

20
21 Regarding claim 22, Bates et al. discloses:

1 *receiving the access control message; automatically converting the first control*
2 *parameter into the virus alert time; comparing the time stamp of the target computer*
3 *content in the list with the virus alert time; and determining the executability of the target*
4 *computer content based on the result of the comparing step (Bates et al., fig. 2, fig. 3,*
5 *fig. 7; see rejections of claims 1 and 2).*

6
7 Regarding claim 23, Bates et al. discloses:
8 applying an anti-virus operation upon the target computer content (Bates et al.,
9 fig. 3).

10
11 Regarding claim 24, Bates et al. discloses:
12 *a second control parameter for specifying types of computer contents that should*
13 *be subject to the access control rule (Bates et al., col. 9, line 62 – col. 10, line 28);*
14 *a third control parameter for specifying an expiration time for the access control*
15 *rule (Bates et al., fig. 7, elem. 217);*
16 *and a fourth control parameter for identifying the access control message (Bates*
17 *et al., fig. 2).*

18
19 Regarding claim 25, Bates et al. discloses:
20 *determining validity of the access control message based on the third control*
21 *parameter (Bates et al., fig. 3);*

22

1 Regarding claim 26, Bates et al. discloses:

2 *determining executability of the target computer content based on the second*
3 *control parameter* (Bates et al., col. 9, line 62 – col. 10, line 28);

4
5 Regarding claims 27 and 28, they are rejected for the same reasons as claims 20
6 and 22, and further because Bates et al. discloses the usage of their system in a
7 network of communicating computers (Bates et al., fig. 1). Communications to a user
8 can be blocked when computer content is deemed to be untrustworthy (Bates et al., col.
9 3, lines 24-27, col. 14, line 6 – col. 15, line 8).

10
11 Regarding claim 29, Bates et al. discloses:

12 wherein the data communication is blocked when the target computer content is
13 time-stamped not before the virus alert time (Bates et al., fig. 3; fig 7).

14
15 Regarding claim 30, Bates et al. discloses:

16 *a firewall module monitoring data communications initiated by a target computer*
17 *content and sending a request to examine the data communications* (Bates et al., fig. 1,
18 elems.20, 30, 50). Bates et al. discloses that the system is useful in a network and it is
19 capable of filtering trustworthy and untrustworthy computer content – thus, acting as a
20 firewall module.

21 *an access control console, for generating an access control message specifying*
22 *an access control rule for blocking data communications of the target computer content*

1 *when said content is time-stamped not before a virus alert time, the access control*
2 *message including a first control parameter for computing the virus alert time (Bates et*
3 *al., fig. 7; fig. 2);*
4 *and an access control module, coupled to the access control console and the*
5 *firewall module, configured to receive the access control message and a request from*
6 *the firewall module, and to compute the virus alert time based on the virus access*
7 *control time and to determine whether the data communication should be blocked*
8 *based on the access control rule (Bates et al., fig. 1, elem. 44, see rejections of claims 1*
9 *and 2).*

10
11 Regarding claim 31, it is a program and computer medium claim implementing
12 the method claim 1, and it is rejected for the same reasons (see also, Bates et al., fig.
13 1).

14
15 Regarding claim 32, Bates et al. discloses:
16 *means for entering a computer virus status mode and for automatically*
17 *recovering a preselected virus access control time (Bates et al., fig. 7);*
18 *coupled to the entering and recovering means, means for computing a virus alert*
19 *time based on the virus access control time (Bates et al., fig. 1, elems. 31, 42, 44),*
20 *and coupled to the computing virus alert time means, means for comparing a*
21 *time stamp of a target computer content with the virus alert time prior to execution of the*
22 *computer content (Bates et al., fig. 1, elem. 42),*

1 *and coupled to the comparing means, means for determining the executability of*
2 *the computer content in response to comparing the time stamp of the target computer*
3 *content with the virus alert time (Bates et al., col. 9, line 56 – col. 10, line 8; col. 11, lines*
4 *12-24). Bates et al. discloses that in response to a comparison, a determination of*
5 *computer content executability is performed. Thus Bates discloses content executability*
6 *determination module, a functional module logically coupled to the system comprising*
7 *an anti-virus module, used to determine the trustworthiness (“executability”) of content.*

8
9 Regarding claim 33, Bates et al. discloses:

10 *means for storing time-stamped executable computer contents (Bates et al., fig.*
11 *1, elem. 46);*

12 *a firewall means for monitoring data communications occurring to the executable*
13 *computer contents (Bates et al., fig. 1, elems. 44, 29, 52).*

14 *means for entering a computer virus status mode and for automatically*
15 *recovering a preselected virus access control time (Bates et al., fig. 7);*

16 *coupled to the entering and recovering means, means for computing a virus alert*
17 *time based on the virus access control time (Bates et al., fig. 1, elems. 31, 42, 44).*

18 *and coupled to the computing virus alert time means, the storing means, and the*
19 *firewall means, means for comparing a time stamp of an executable computer content*
20 *with the virus alert time to determine whether the data communication occurring to the*
21 *executable computer content should be blocked (Bates et al., fig. 1, elem. 44, 42).*

22

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bates et al., U.S. Patent 6,721,721 B1 in view of Symantec, "Norton AntiVirus Corporate Edition".

Regarding claim 11, Bates et al. discloses that viruses can be found in email attachments, and that it is well known in the art for antivirus programs to have the capability for performing antivirus processing on emails and email attachments (Bates et al., col. 1, lines 35-63). Bates et al. discloses an antivirus program or module for performing such antivirus processing (Bates et al., fig. 1, elems. 44, 52). Bates et al., however, does not disclose the details of the antivirus processing for emails and email attachments. Specifically, Bates et al. does not disclose that the antivirus program or module removes the computer content from the E-mail body, and denies execution of the computer content.

Symantec discloses an antivirus program and the details of how the program performs antivirus processing upon an email with an attachment. Symantec discloses that the antivirus program scans content attached to an email body and removes such

content if it is found to contain a virus, thus, denying execution of the content
(Symantec, page 15, par. 2; page 22, "Managing Realtime Protection").

It would have been obvious for one of ordinary skill in the art to combine the
details disclosed by Symantec for the antivirus processing of emails with the system of
Bates et al. because the system of Bates et al. discloses an antivirus program capable
of performing antivirus processing for processing of emails.

Response to Arguments

Applicant's arguments filed 2/6/2006 have been fully considered but they are not
persuasive.

Applicants argue primarily that:

(i) *Bates, on the other hand, requires that the user manually enter time
parameters. See, e.g., Bates, Figure 7, item 214. The programmatic computation of the
alert time is distinct over a system in which the user must key in time parameters, at
least in that it saves effort and enables much faster and more extensive processing than
can be achieved in Bates.*

*This is not a trivial distinction, as it enables the system to run at an efficiency and
scale which is simply not possible where time parameters must be entered by a human
being. (Remarks, pg. 11)*

1
2 The examiner notes that the applicant's representative has mistakenly alleged a
3 distinction of the claimed invention over prior art. Specifically, the applicant's
4 representative incorrectly asserts that Bates et al. requires a user who enters time
5 parameters into the system, whereas the present invention does not. In response, the
6 examiner respectfully directs the applicant's representative to the applicant's own
7 disclosure (i.e. pars. 9-11, 68, 69). Throughout the applicant's own disclosure, a user is
8 disclosed as entering time parameters, which are then used to formulate a rule (i.e. see
9 par. 9). This is not a distinction over Bates et al. as alleged by the applicant's
10 representative, as Bates et al. similarly formulates a rule based upon the time
11 parameters entered by the user. Furthermore, the invention as claimed, "computing",
12 does not distinguish over Bates et al. (See rejection of claim 1).

13
14 (ii) *Additionally, each independent claim recites determining the executability of*
15 *computer content based on either "comparing a time stamp of [the] content with the*
16 *virus alert time" or on "a control rule," prior to execution of the computer content. Bates*
17 *does not determine whether content is safe to execute based on such criteria, but*
18 *simply looks at a timestamp to determine whether the file that is being inspected has*
19 *been changed. If the file has been changed, Bates can then execute the additional step*
20 *of scanning the file for viruses. It is only as a result of the subsequent scanning*
21 *step that it is determined whether the content can be safely executed. See. e.g., Bates,*
22 *column 12, lines 59-65.*

1 *Once again, such a distinction is not trivial. Bates can determine only which files*
2 *need to be scanned for viruses, whereas the present invention, as recited by the*
3 *independent claims, is capable of determining which content is safe to execute, absent*
4 *an additional, processor intensive, and lengthy virus scan of each file that has been*
5 *touched. (Remarks, pg. 11, 12)*

6
7 In response to this argument, the examiner respectfully points out that the
8 applicant's representative has mischaracterized the reference of Bates et al. Bates et
9 al., as discussed in the above rejections, makes a determination of file trustworthiness
10 based upon the comparison of the virus status information (i.e. timestamp) associated
11 with the file. Bates et al. does not disclose a required and subsequent virus scan of
12 each "file that has been touched" (Bates et al., col. 11, lines 1-24).

13
14 (iii) *Claim 11 depends upon amended claim 1, which, as discussed above, is*
15 *patentable.*

16 *Furthermore, there exists no motivation to combine Bates and Norton.*
17 (Remarks, pg. 12)

18
19 In response the examiner points out to the applicant's representative that claim 1
20 has been rejected.

1 Furthermore, regarding the argument of the applicant's representative that there
2 exists no motivation to combine Bates and Norton, the examiner points out that the
3 applicant's representative provides no basis for such an allegation.

4
5
6
7 **Conclusion**

8
9 The prior art made of record and not relied upon is considered pertinent to
10 applicant's disclosure:

11
12 **See Notice of References Cited**

13
14
15 A shortened statutory period for reply is set to expire 3 months (not less than 90
16 days) from the mailing date of this communication.

17 Any inquiry concerning this communication or earlier communications from the
18 examiner should be directed to Jeffery Williams whose telephone number is (571) 272-
19 7965. The examiner can normally be reached on 8:30-5:00.

20 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
21 supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
AU: 2137



EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER